

FILED

MAR 31 2016

UNITED STATES DISTRICT COURT

for the
Eastern District of North CarolinaJULIE RICHARDS JOHNSTON, CLERK
US DISTRICT COURT, EDNC
BY BEH DEP CLK

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)A pink SanDisk 8 GB external memory drive and the residence located at
1133 Wellons Drive, Fayetteville, NC 28304, including any detached
structures thereto, as well as authorizing the forensic examination of
computers and related computer equipment.Case No. 5:16-mj-1271-JG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):

See Attachment A and the Affidavit, both incorporated herein by reference

located in the Eastern District of North Carolina, there is now concealed (identify the
person or describe the property to be seized):

See Attachment B and the Affidavit, both incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. Section 2251(a) and (c)(2)
(b); 18 U.S.C. 2252A(a)(2)(A); 18
U.S.C. 2252A(a)(5)(B) and (b)(2)

Offense Description
Sexual exploitation of children; receipt and distribution of,
conspiracy to receive and distribute, and attempt to receive
and distribute child pornography; possession of child pornography

The application is based on these facts:

See Affidavit of FBI SA Eugene Vinson and Attachments A and B all incorporated herein by reference

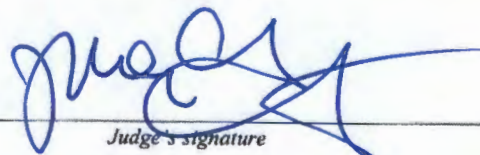
- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

On this day, Eugene Vinson
appeared before me via reliable electronic means, was
placed under oath, and attested to the contents of this
Application for a Search Warrant.Date: 31 March 2016City and state: Raleigh, North Carolina

Applicant's signature

Eugene Vinson, FBI Special Agent

Printed name and title



Judge's signature

James E. Gates, United States Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the Eastern District of North Carolina

In the Matter of the Search)
of:)
) Case No.
A pink SanDisk 8 GB external)
memory drive and the residence)
located at 1133 Wellons Drive,)
Fayetteville, NC 28304,)
including any detached)
structures thereto, as well as
authorizing the forensic
examination of computers and
related computer equipment.

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Special Agent Eugene Vinson, having been first duly sworn, do hereby depose and state as follows:

1. I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant. I have been employed as a Special Agent of the FBI since February 2013, and am currently assigned to the Fayetteville Resident Agency of the Charlotte Division. I am primarily responsible for investigating violent and white collar crime in the Fayetteville area. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography. I have gained experience through training at the FBI and everyday work relating to conducting these types of

Page 1 of 24

JMK

[Handwritten signature]

investigations. I have received training in the area of child pornography and child exploitation. In relation to this training, I have observed numerous examples of known child pornography (as defined in 18 U.S.C. § 2256) in various forms, to include computer media.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2251(a) and (c)(2)(b) (sexual exploitation of children)¹; 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography)²; and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or

¹ 18 U.S.C. §§ 2251(a) and (c)(2)(b) prohibits a person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e) and the person transports such visual depiction to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail.

² 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer

attempted access with intent to view child pornography)³, are located within 1133 Wellons Drive, Fayetteville, North Carolina 28304 (hereinafter the "SUBJECT PREMISES"). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES and a pink SanDisk 8GB external memory drive, as further described in Attachment A, incorporated herein by reference, which is located in the Eastern District of North Carolina.

3. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

4. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have

³ 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

JMK

received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent (SA) with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE⁴

5. HUGUES LAGADEC is the subject of a French investigation related to allegations that he sexually assaulted his minor granddaughter (hereinafter referred to as "the Victim"), while visiting his family in France in 2012. Specifically, the allegations concerned punitive provisions under French law regarding sexual assault on a minor under 15 years and corruption of a minor. Through a Mutual Legal Assistance Treaty (MLAT), the Government of France requested

⁴ A section defining terms used within this affidavit is provided at page 18.

that LAGADEC be interviewed regarding the allegations.

6. On 26 February 2016, your Affiant approached LAGADEC at his residence located at 1133 Wellons Drive, Fayetteville, NC. LAGADEC initially stated that his English was not good; therefore your Affiant obtained the assistance of an FBI translator to assist via telephone. The FBI translator was placed on speakerphone and for both parties, translated all conversation between your Affiant and LAGADEC.

7. Your Affiant requested to speak with LAGADEC, who agreed and invited your Affiant into his home. While sitting at LAGADEC's kitchen table, your affiant explained that there had been an allegation made against LAGADEC by his granddaughter and that your Affiant wished to speak with him about it. LAGADEC consented to answering questions regarding the allegation. Although the interview was non-custodial, before proceeding, LAGADEC was first advised of his rights under French law pursuant to the provisions of the MLAT request.⁵

8. LAGADEC was shown a series of sexually explicit chat

⁵ This included first orally informing LAGADEC of the below rights and then obtaining his signature on a form that listed the following rights to:

- Contact a family member or the consular authorities;
- Be examined by a doctor;
- Be assisted by an attorney;
- Be assisted by an interpreter;
- Make submissions to appropriate authorities if placed in custody
- Make a statement, to answer questions, or to remain silent

messages, which LAGADEC admitted to exchanging with the Victim. LAGADEC advised that these chat messages were still saved on one of his computers. LAGADEC was also shown nude photos of himself that had been sent to the Victim and which were recovered by the French Government. LAGADEC identified himself as the individual in the photos and admitted to sending them to the Victim. LAGADEC stated that he had accidentally sent these to the Victim and that he had instructed the Victim to delete these photos.

9. Upon being confronted with the language of some of the chats which were sexually explicit, LAGADEC claimed that he had been attempting to gather evidence against his granddaughter. When asked why he would need to do this, he claimed that his 14 year old granddaughter had raped him. He claimed that he awoke one night while having an erotic dream and that his granddaughter was naked on top of him. He claimed that she forced him to have intercourse with her.

10. LAGADEC offered to show your Affiant where the chat messages were located on his computer. LAGADEC then agreed to allow your Affiant to conduct a cursory exam of the computers present in the house and LAGADEC signed a "Consent to Search" form. At least three computers and various memory drives and devices were observable in the home. Peer to peer programs were also noted on at least one of the computers which LAGADEC stated

he utilized. At one point, while searching for the chat messages, LAGADEC accessed a folder that your Affiant observed as potentially containing the saved chat messages as well as a folder with family photos. Your Affiant noticed that the many of the photos seemed to be of the Victim in natural and various settings. Your Affiant requested whether he could take a copy and LAGADEC then inserted a pink SanDisk 8GB memory drive and saved the data to the memory drive. He then voluntarily provided the memory drive to your Affiant.

11. On 22 March 2016, the FBI began preparing a copy of the SanDisk 8GB memory drive to be sent as part of the response to the MLAT from the Government of France. During the preparation, a forensic image of the device was created. The digital forensic examiner noted there were additional images on the drive located in the unallocated space. The images did not appear to be what LAGADEC had shown Affiant during his interview. The first image was a full body nude photo of what appeared to be the victim. The next image was of the victim performing oral sex on an adult male. While the adult male subject's face is not seen in the photo, the visible body structure and genitalia appeared to be similar to the photos shown to LAGADEC during his interview which he self-identified. Additionally, Affiant noted the body shape and hair appeared to

JMK

gt

be similar to that of LAGADEC. At this point, all forensic examination of the thumb drive was halted.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO
ACCESS WITH INTENT TO VIEW [AND/OR COLLECT, RECEIVE,
DISTRIBUTE OR ADVERTISE] CHILD PORNOGRAPHY

12. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view and/or possess, collect, receive, images of child pornography:

- a) Individuals who access with intent to view and/or possess, collect, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b) Individuals who access with intent to view and/or possess, collect, and receive, child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c) Individuals who access with intent to view and/or possess, collect, and receive child pornography almost

always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

- d) Likewise, individuals who access with intent to view and/or possess, collect, and receive, pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.
- e) Individuals who access with intent to view and/or possess, collect, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f) Individuals who access with intent to view and/or possess, collect, and receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

13. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

14. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store 32 gigabytes of data or more, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

15. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable,

or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

16. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the

JMK

computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

17. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

18. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

19. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can

JMK



be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

20. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the

stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

21. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

22. Furthermore, because there is probable cause to

believe that the computers and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

23. Based upon my training, experience, and information obtained from other law enforcement officials familiar with child exploitation crimes, I know that when an individual uses a computer to download child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I know that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense. There is probable cause to believe that the contraband images (child pornography) will be located on the hard drives of the suspect's computers and on any digital media storage devices located within the residence mentioned in Attachment A, which will

constitute evidence, fruits, and instrumentalities of child exploitation crimes, including the receipt, distribution, and/or collection of child pornography.

24. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

- a) The process of searching the digital files contained within digital media storage devices at the scene can take a long time to complete. To be certain the digital storage devices in question do not contain any contraband materials, law enforcement officers would have to examine every one of what may be thousands of files on a digital storage device. This process could take a long time. Taking too much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress therefore denying the suspect(s) access to their home or business for an extended amount of time. If the search took hours or days, the intrusion would

JMK

JA

continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible.

- b) Technical requirements for searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

25. In light of these concerns, I hereby request the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some, or all of the evidence described in the warrant, and conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

DEFINITIONS

Page 17 of 24

26. The following definitions apply to this Affidavit and attachments hereto:

- a. **"Chat"** refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- b. **"Child Erotica,"** as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.
- c. **"Child Pornography,"** as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- d. **"Computer,"** as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
- e. **"Computer Server" or "Server,"** as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the

user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

- f. **"Computer hardware,"** as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- g. **"Computer software,"** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h. **"Computer-related documentation,"** as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- i. **"Computer passwords, pass-phrases and data security devices,"** as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security

devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- j. **"File Transfer Protocol" ("FTP")**, as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
- k. **"Hyperlink"** refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- l. **The "Internet"** is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- m. **"Internet Service Providers" ("ISPs")**, as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line

("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- n. **"Internet Protocol address" or "IP address"** refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- o. **Media Access Control ("MAC") address.** The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.
- p. **"Minor"** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- q. **"Peer to Peer"** P2P file sharing networks allow users to download and upload files from other users, referred to as peers, on the Internet, typically from within an application running on their local computer that

follows a particular protocol. P2P networks consist of a set of Internet peers communicating and sharing files via a specific protocol. The primary goal of every P2P file sharing system is to support efficient distribution of content shared among peers. Many P2P systems also directly support content searches by peers, and some allow a direct browsing of the files that a remote peer makes available.

- r. **The terms "records," "documents," and "materials,"** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- s. **"Secure Shell" ("SSH"),** as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.
- t. **"Sexually explicit conduct"** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
- u. **"URL"** is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made

of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

v. **"Visual depictions"** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

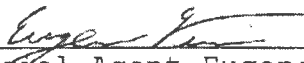
w. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP");

CONCLUSION

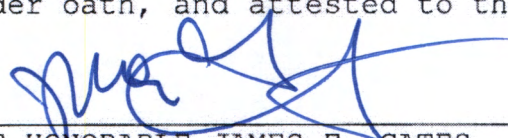
27. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

28. Your Affiant is aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated

in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.


Special Agent Eugene Vinson,
Federal Bureau of Investigation

On this 31 day of March 20 16, Special Agent Eugene Vinson appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit.


THE HONORABLE JAMES E. GATES
UNITED STATES MAGISTRATE JUDGE

JMK

ATTACHMENT A

PROPERTY TO BE SEARCHED

LOCATION: 1133 Cardiff Drive, Fayetteville, North Carolina
("Subject Premises"); to include any appurtenances and curtilage to the Subject Premises and any storage units/outbuildings and vehicles located on the Subject Premises and curtilage.

The Subject Premises is a single story family dwelling with a red brick front and white siding. The roof has reddish shingles and white trim around the windows. The driveway is located to the right of the house when facing the building. The number 1133 is visible on the front of the building on the door to the right as you face the house from the road. See Picture below.



[Handwritten signature]

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

This warrant authorizes (i) the search of the property identified in **Attachment A** for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

- (a) evidence of violations of Title 18 U.S.C. §§ 2252 and 2252A, Sexual Exploitation of Minors and Material Constituting Child Pornography ("subject violations"); or
- (b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or
- (c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be searched for and seized include the following:

1. Computer(s), computer hardware¹, software², related documentation³, passwords and data security devices⁴,

¹ Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, telephones and other mobile or portable devices, video gaming systems, tablets, music/media players, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

² Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.


³ Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.



videotapes, video recording devices, video recording players, monitors and or televisions, and data were instrumentalities of and will contain evidence related to this crime.

2. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, § 2256(8).
3. Any and all correspondence identifying persons transmitting, through interstate commerce including by United States Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2).
5. Any and all records, documents, invoices and materials that concern any accounts with any Internet Service Provider.
6. Any and all cameras, film, or other photographic equipment.
7. Any and all visual depictions of minors.
8. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States Mails or by computer, and visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2).
9. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2).

⁴ Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.



10. Any and all documents, records, or correspondence pertaining to occupancy at Subject Premises (1133 Wellons Drive, Fayetteville, NC 28304).
11. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2). Any of the items described in paragraphs 1 through 11 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form.

